

Decentralized Identity

at Microsoft



2018: Incubation hypothesis

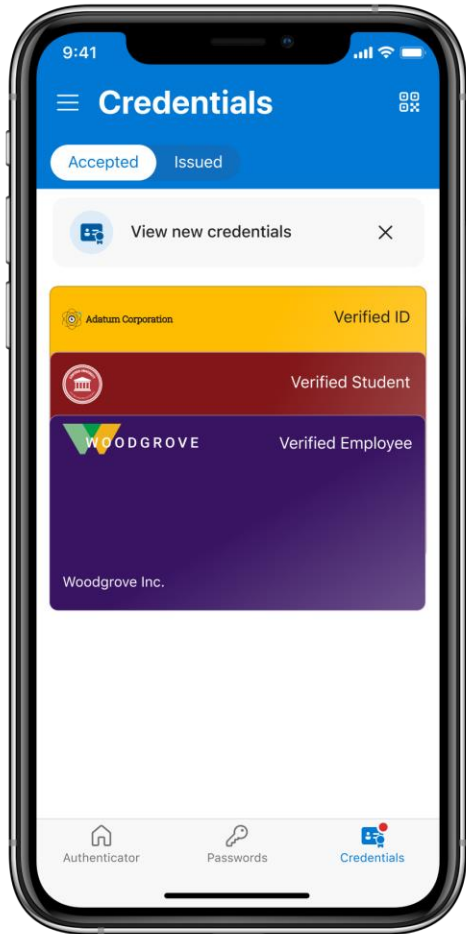
2022: First Release!

Each of us needs **digital identity we own and control**, one which securely and privately stores **all elements of our digital identity**.

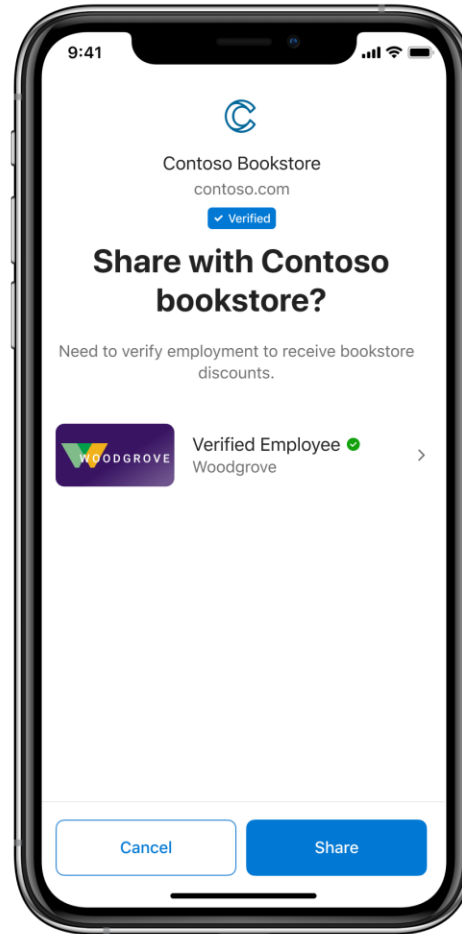
This self-owned identity must **seamlessly integrate into our lives** and give us **complete control over how our identity data is accessed** and used.



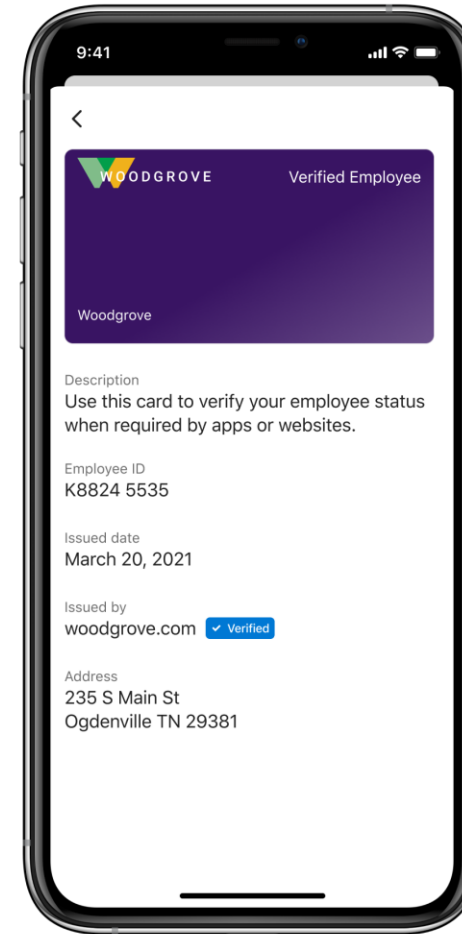
Entra Verified ID: a better way to verify



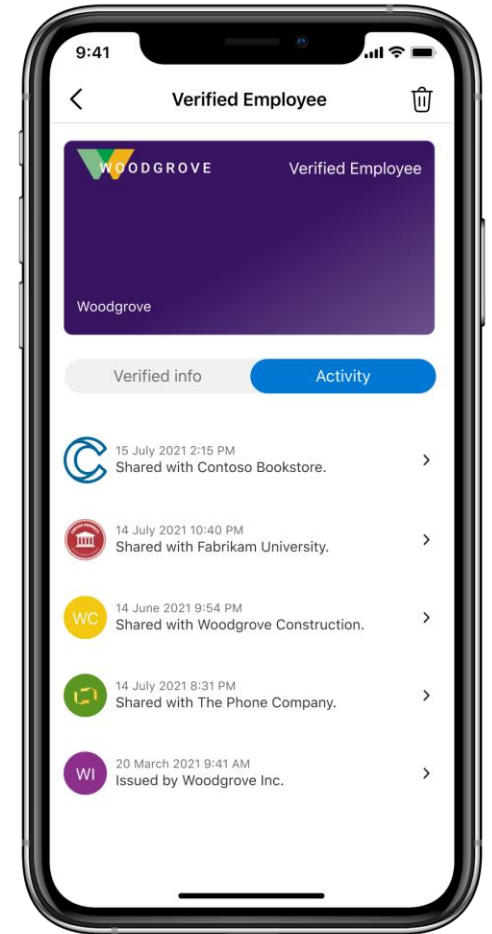
Easy to use and secure



Verifiable

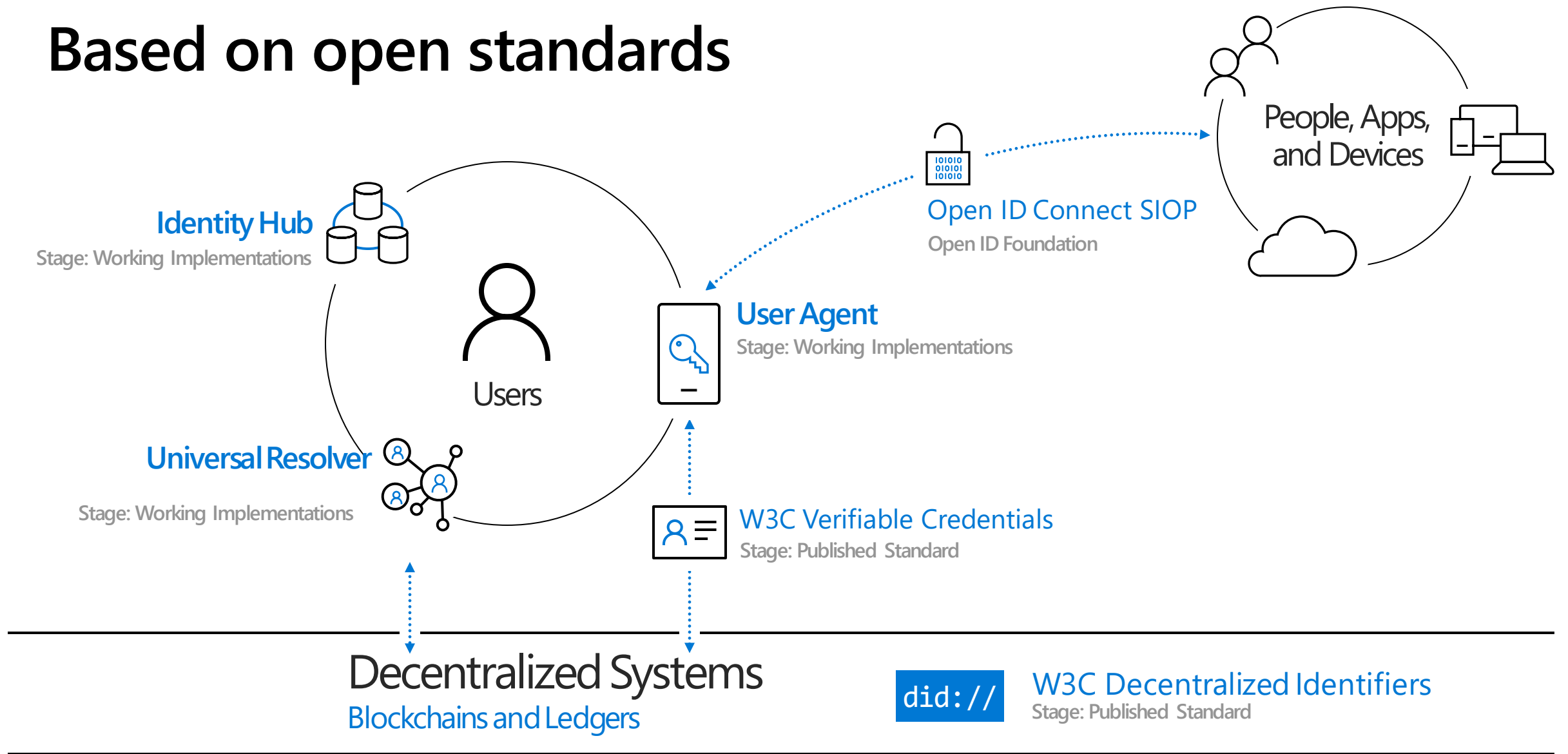


Transparent

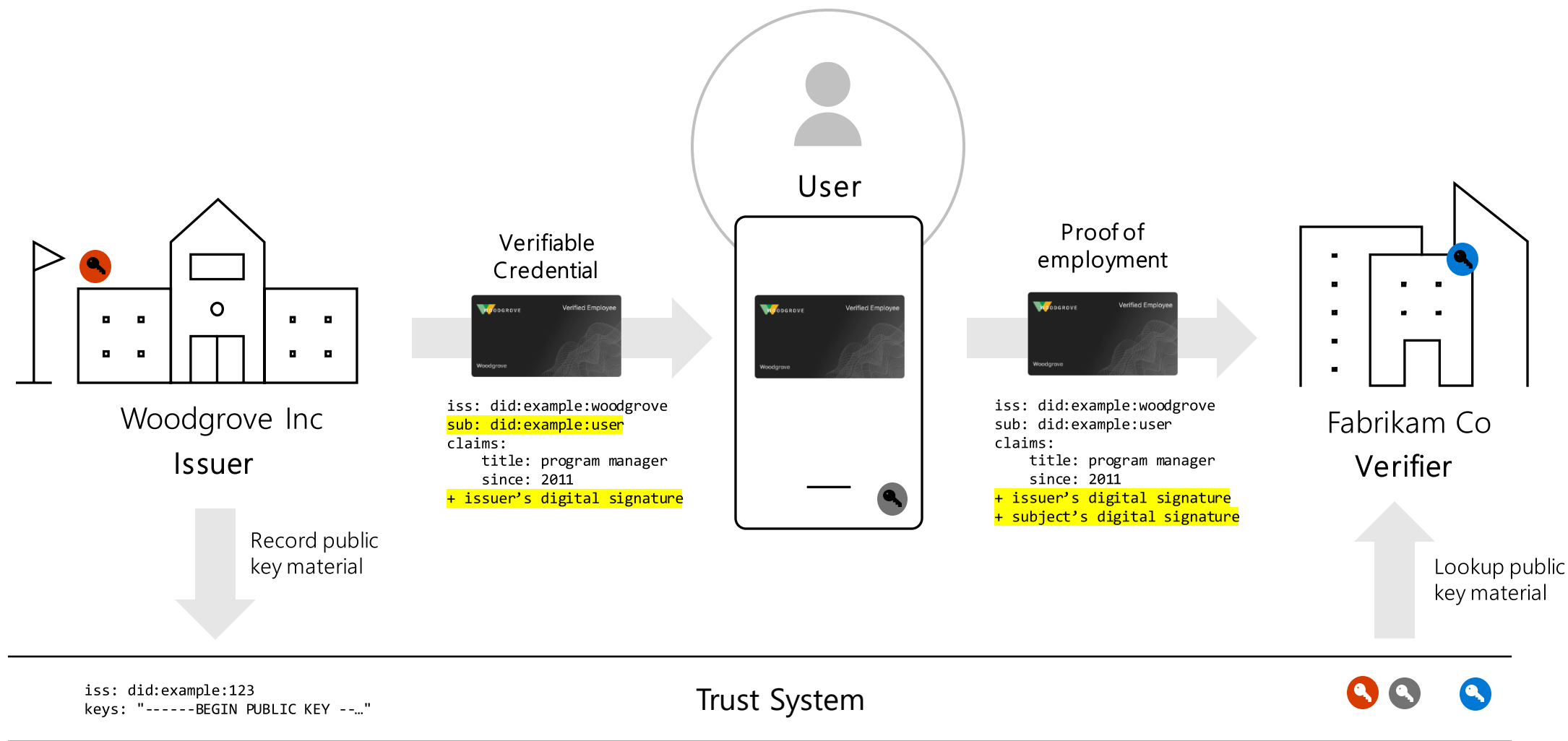


Convenient

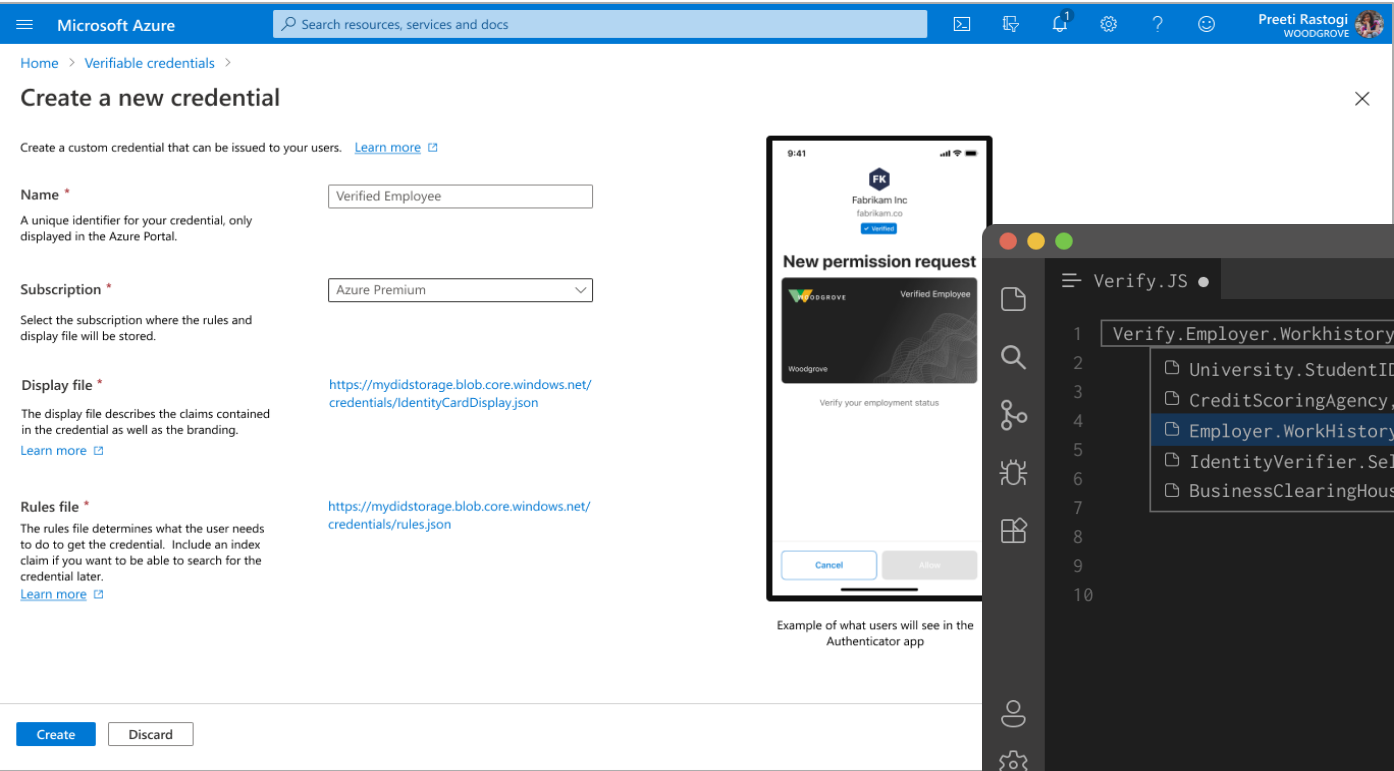
Based on open standards



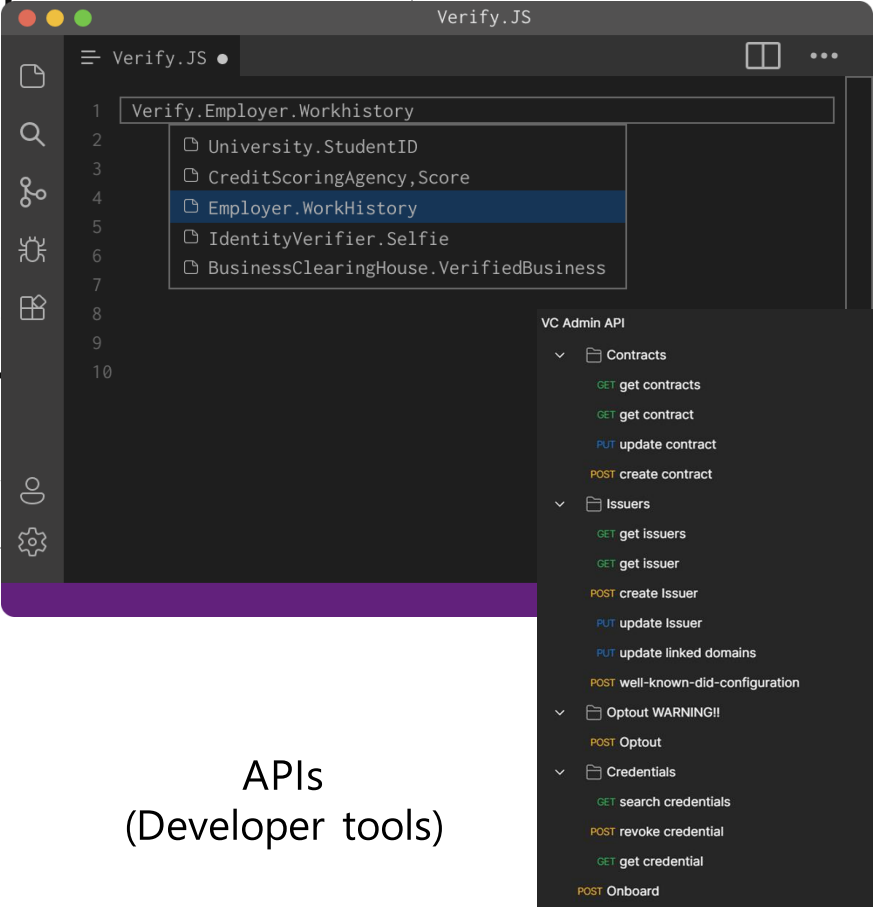
How does this work?



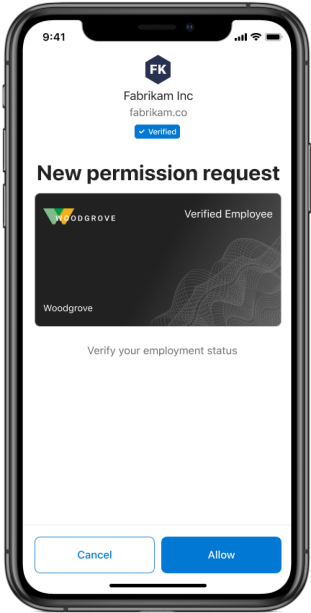
Decentralized Identity Platform by Microsoft



Issuer & Verifier interface
(Entra Verified ID)



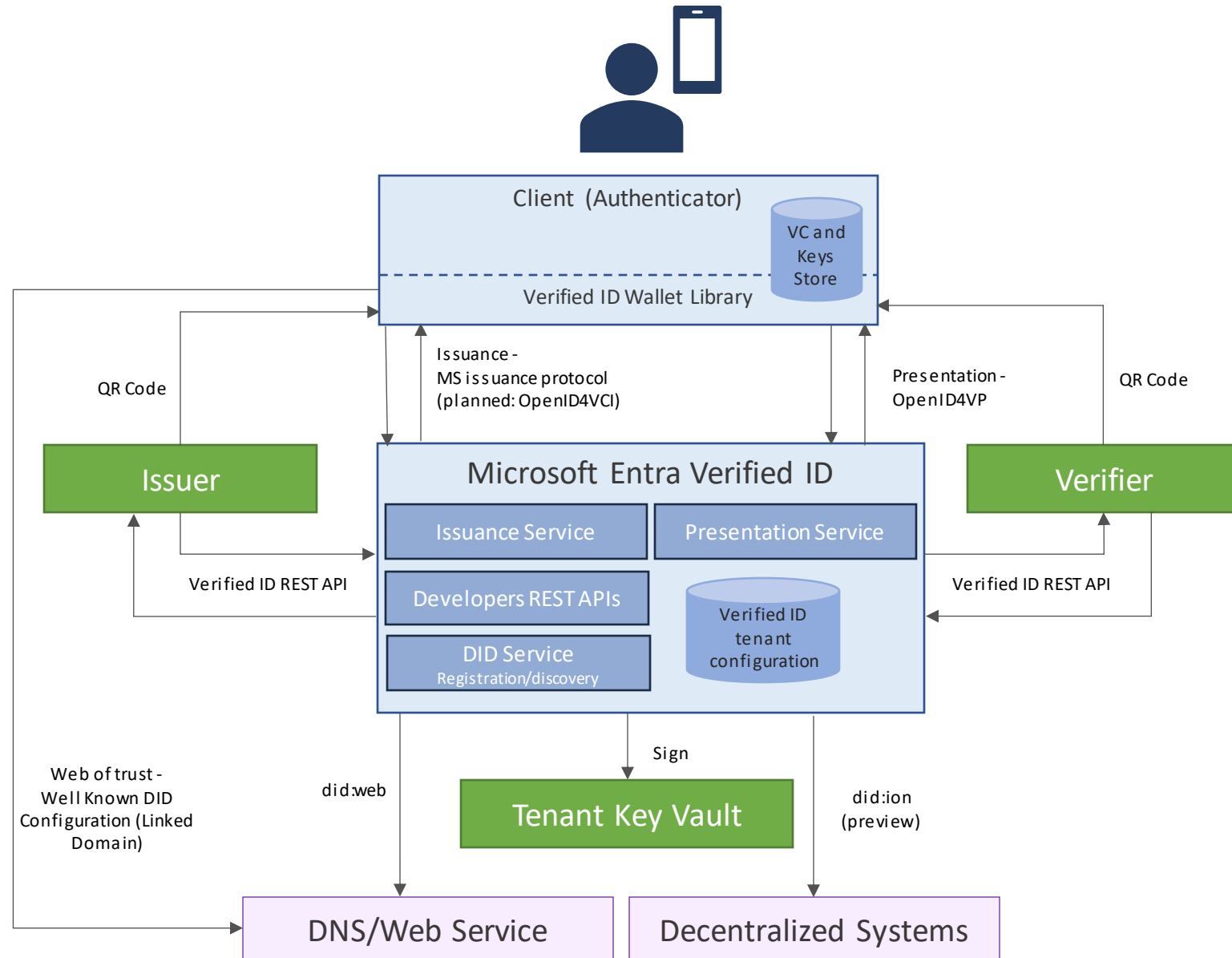
APIs
(Developer tools)



Wallet library
(Microsoft Authenticator)

Architecture goals:

1. Decentralized system to request and verify credentials at scale
2. Ensure interoperability as standards and partnerships evolve
3. Simple APIs to ensure consistent interactions that abstract standards and cryptography





Verified ID

Enable more secure interactions while respecting privacy with an industry-leading global platform.

Fast remote onboarding

Validate identity information for trustworthy self-service enrollment and reduced time-to-hire.

More secure access

Quickly verify an individual's credentials and status to grant least-privilege access with confidence.

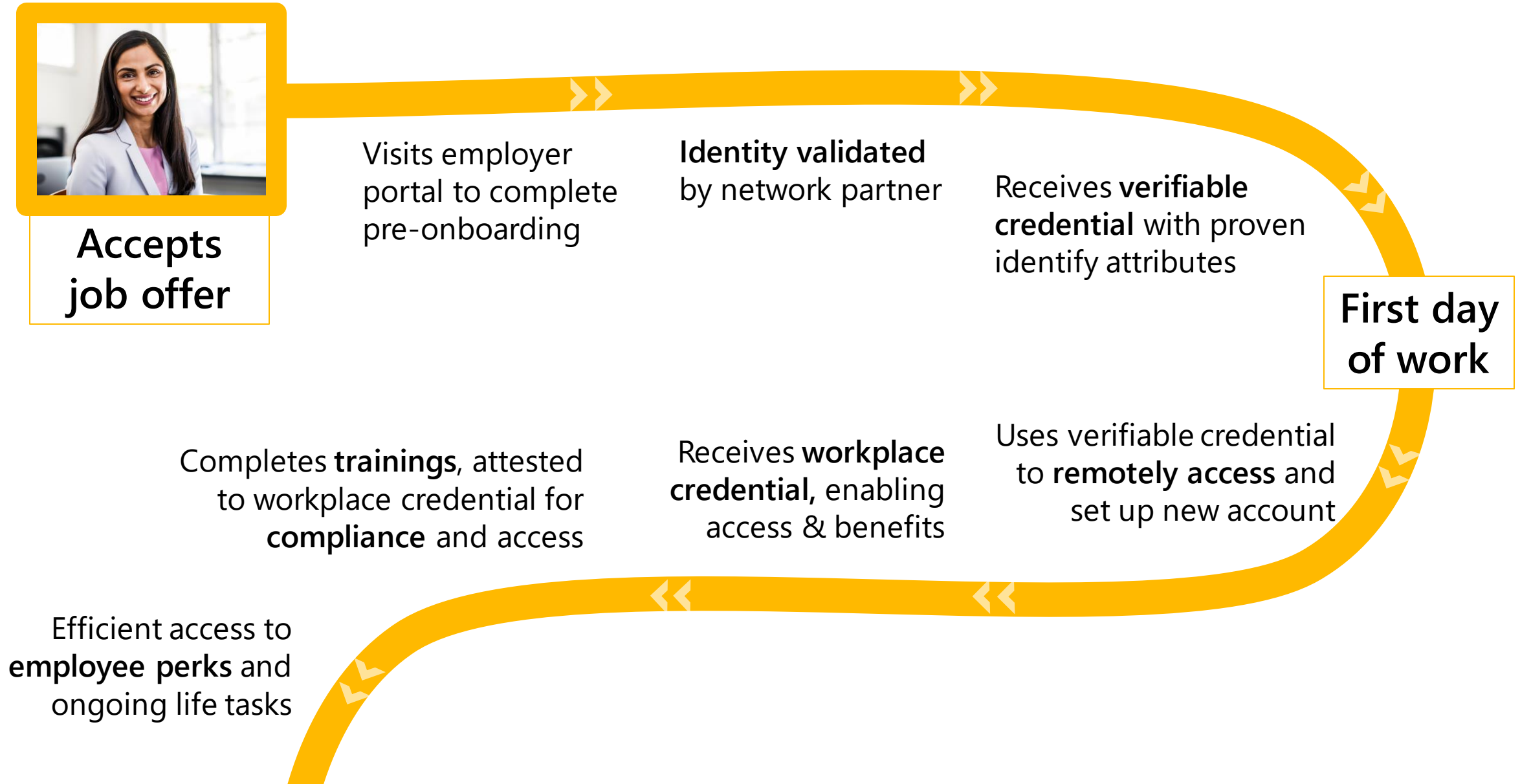
Easy account recovery

Replace support calls and security questions with a streamlined self-service process to verify identities.

Custom business solutions

Easily build solutions for a wide range of use cases with our developer kit, APIs, and documentation.

Ongoing value journey: Worker productivity



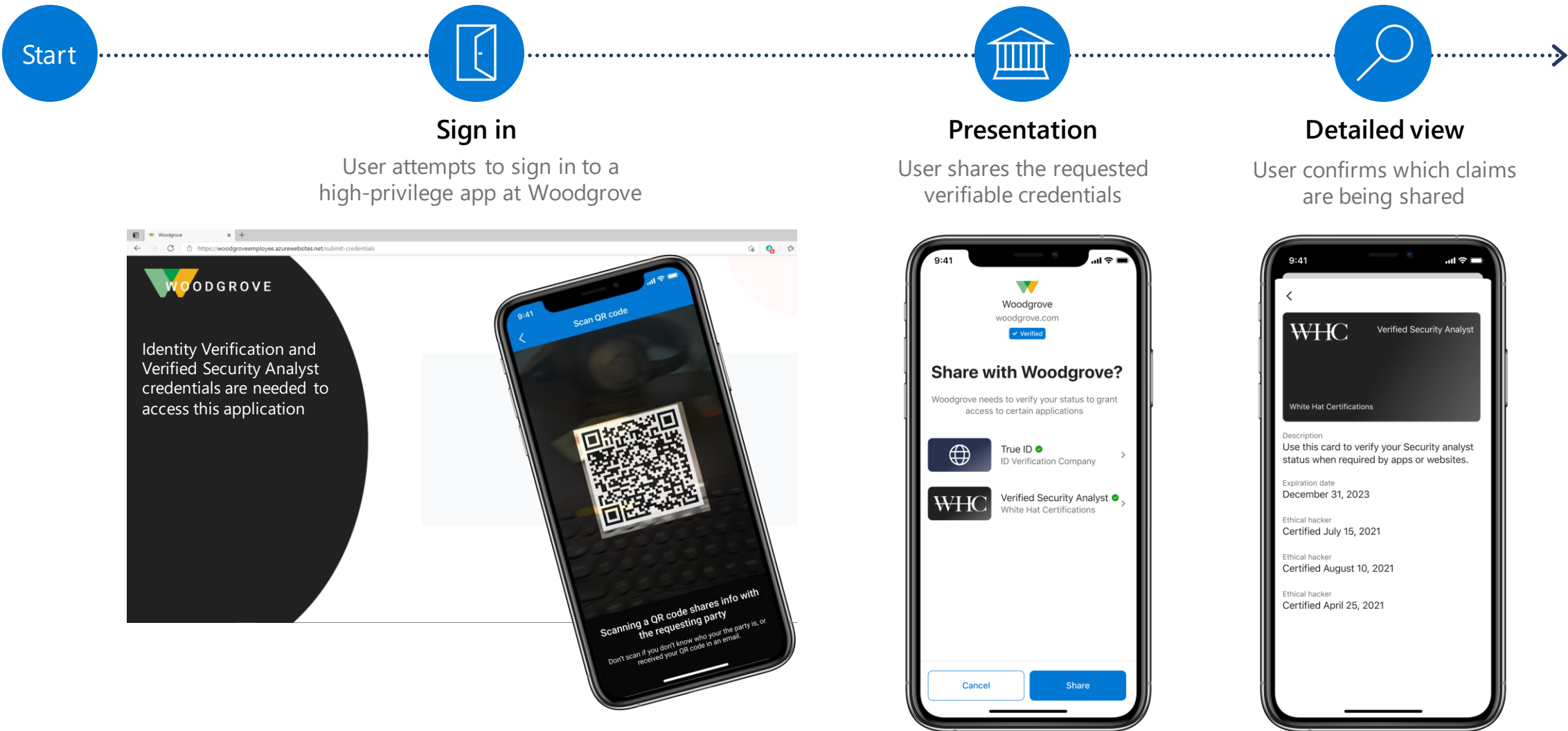
Demonstration: ID verification based on open standards



<http://aka.ms/diddemo>

Secure access to applications

Quickly verify credentials and get access to sensitive resources that have advanced security requirements



Northwind Airlines

Home

Identity Challenge

Lounge Access

Identity Challenge

Prove your identity by pressing the **Verify Credential** button and present your membership card

Waiting for user to present VC

Scan with Microsoft Authenticator or Custom Wallet

© 2023 - Northwind Airlines - Privacy

18:47

Verified IDs

RG Verified Employee

Northwind Miles Club

Verified Employee

Verified Employee

Verified Employee

Microsoft

Authentication

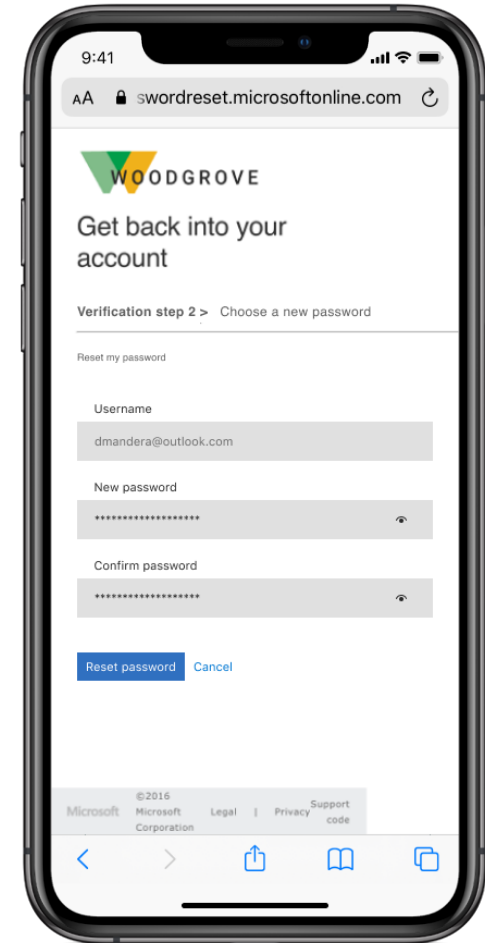
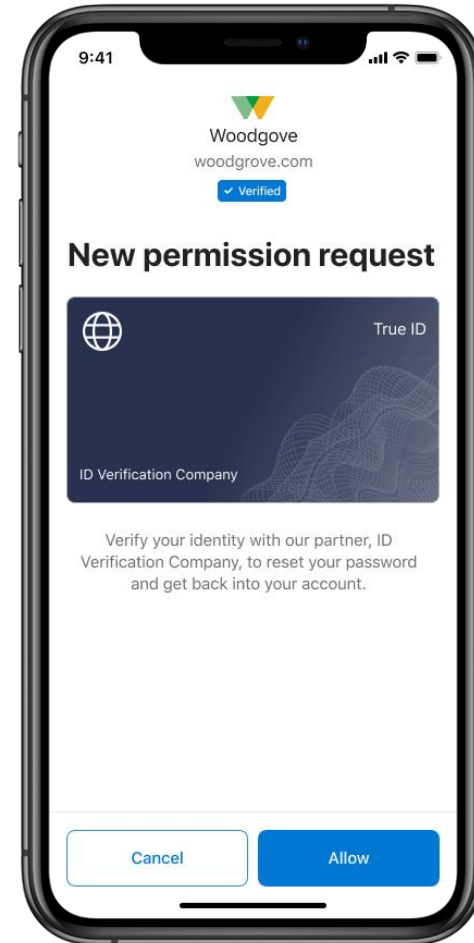
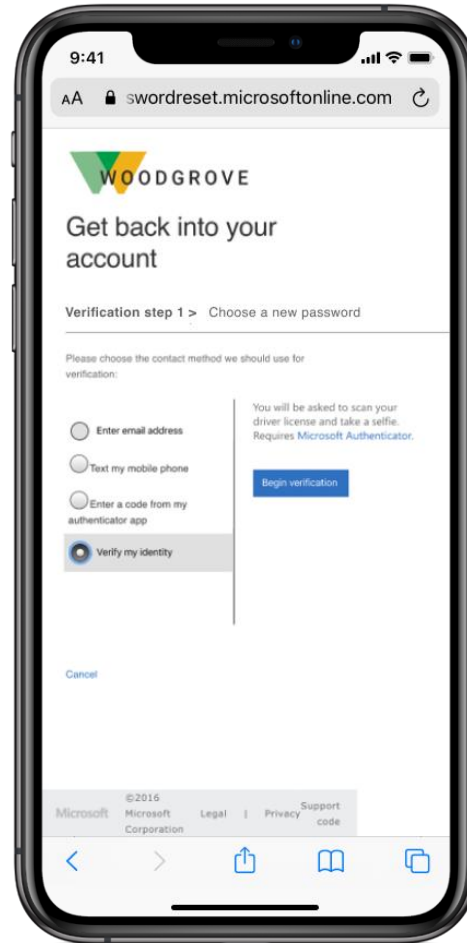
Passkeys

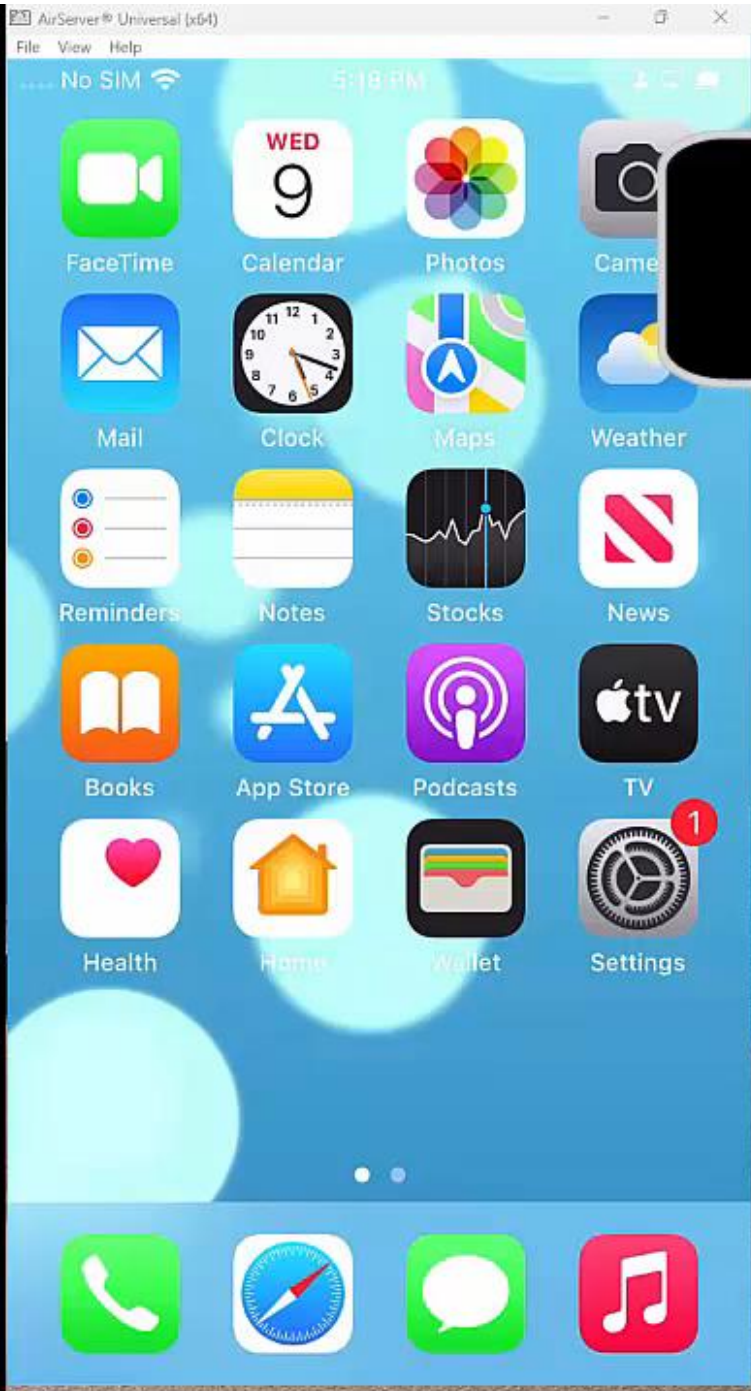
Address

Verified IDs

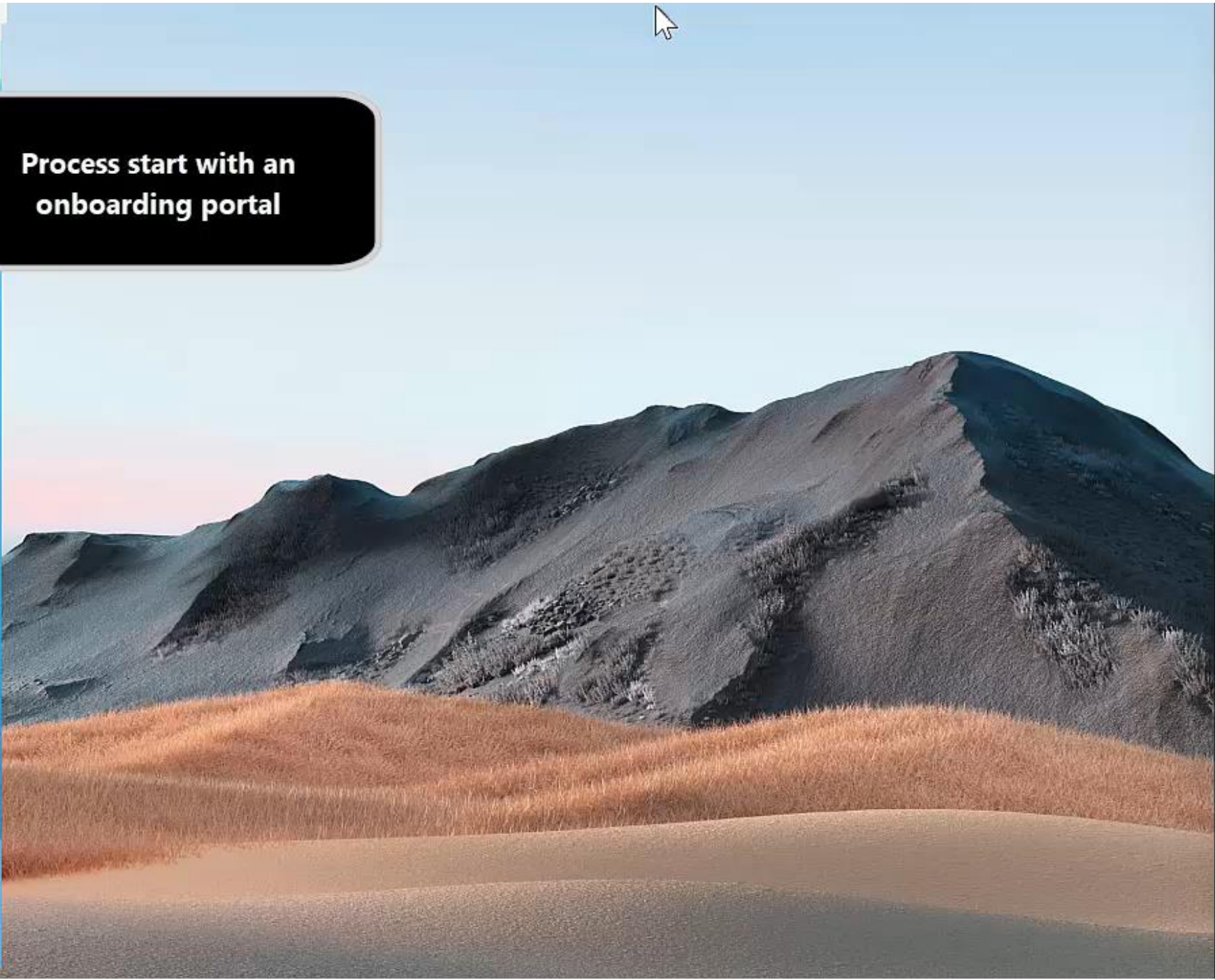
Account Recovery

Reduce support phone calls and security questions with a simpler, more secure process to verify identity.





Process start with an onboarding portal



Entitlement Management with Verified ID



Verify granular attributes from a wide set of issuers



Reduce approval fatigue



Automatically revoke access when VC is revoked



Better compliance posture

Microsoft Azure Search resources, services and docs

Identity Governance > Create a policy >

Create a policy

Configure policy Approval Requestor information Lifecycle Review

Choose which users or applications can request access. By default, admins can always assign users to the access package. You can also designate other users or applications to request access on behalf of the users and applications within the scope of the policy.

Users who can get access ⓘ

For users not in your directory

☐ Specific connected organizations
+ Add directories

☐ All configured connected organizations

☒ All users (all connected organizations + any new external users)

Users who can make requests ⓘ

☒ Admin
Admin can't be turned off because admins will always be able to assign users to an access package

☒ Self

☐ Manager

☐ Internal Sponsor

☐ External Sponsor

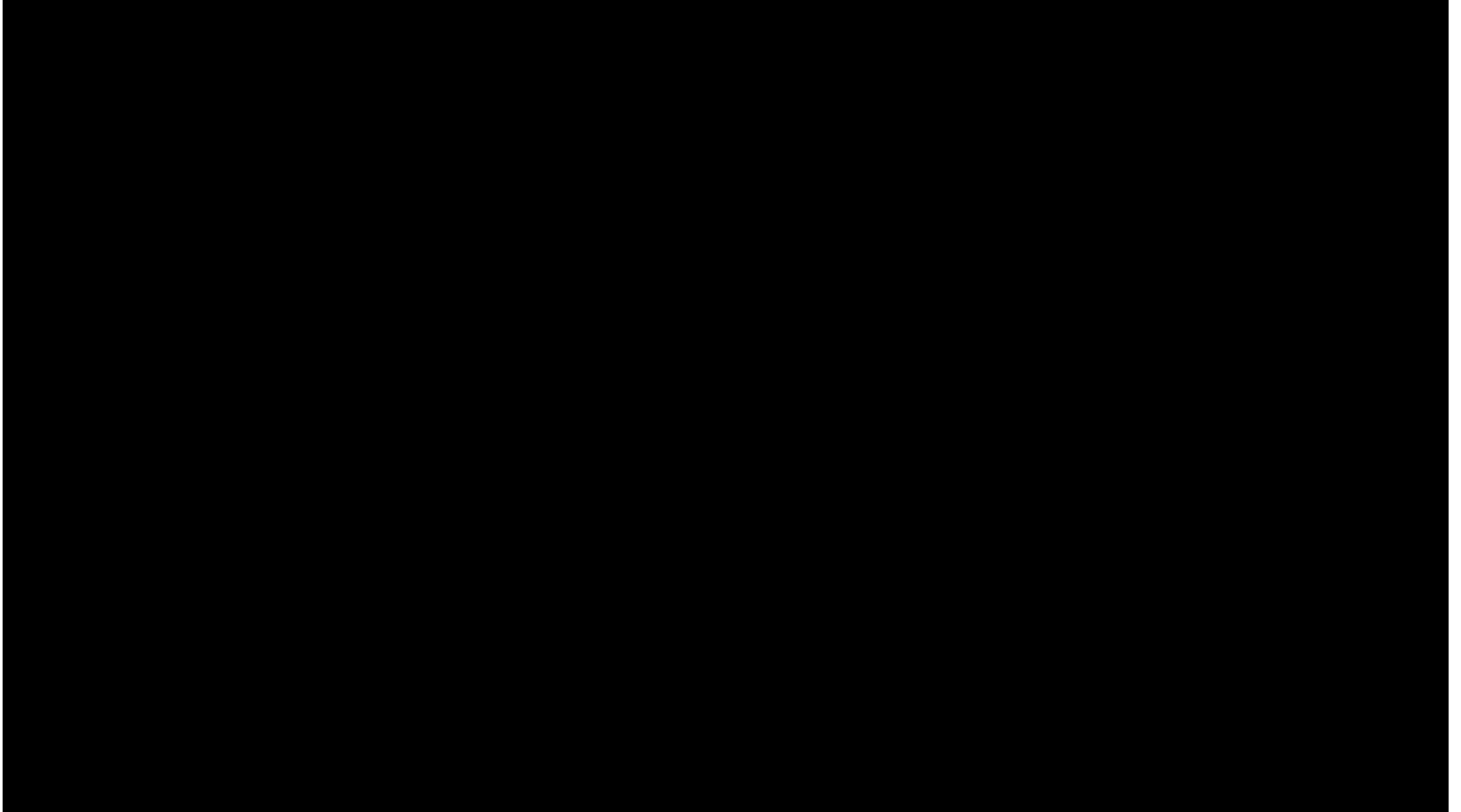
Users to provide Verifiable Credentials

Add

Issuer	Domain	Credential types	Claims
--------	--------	------------------	--------

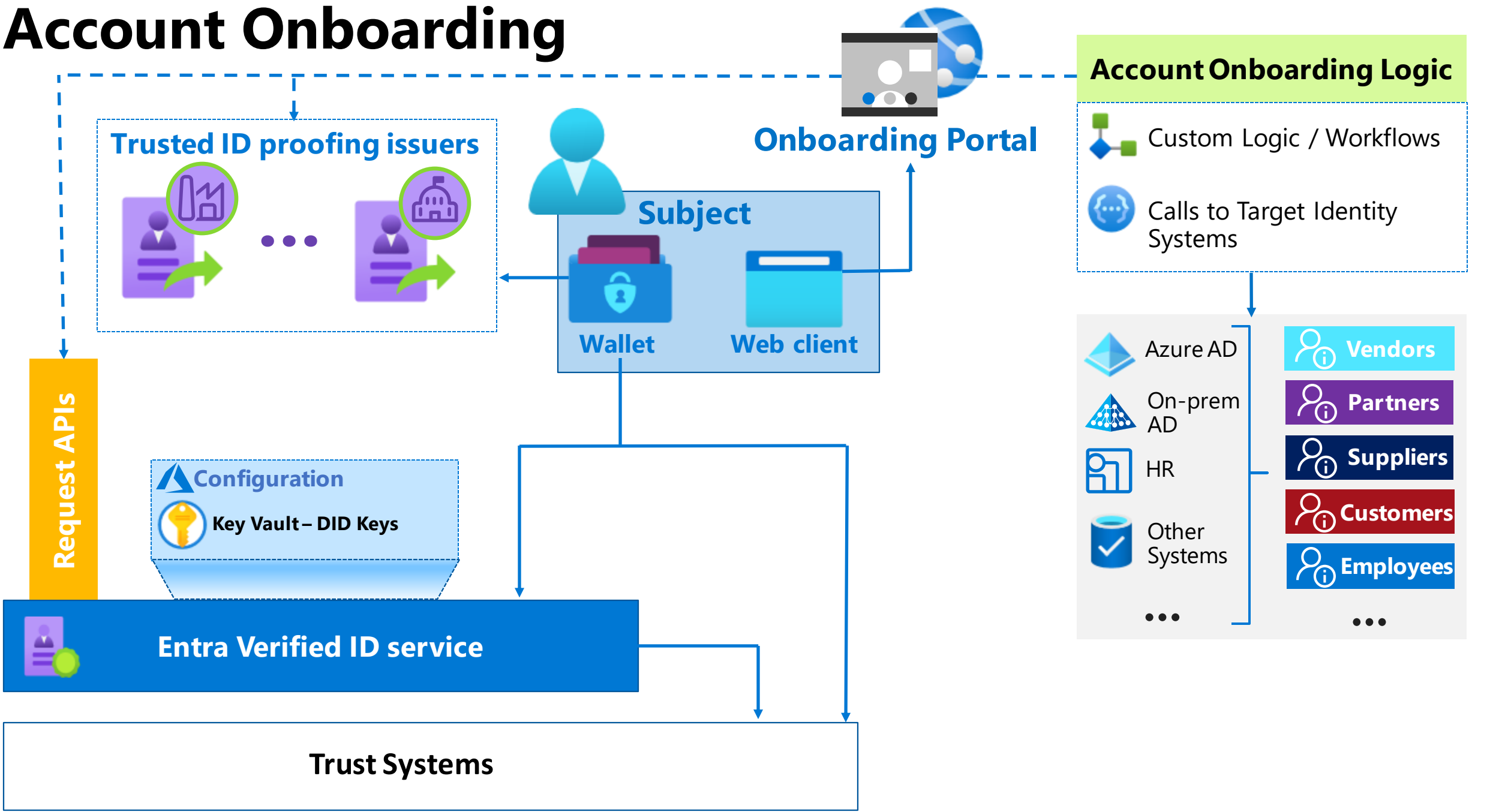
Previous Next

Let's see it in action

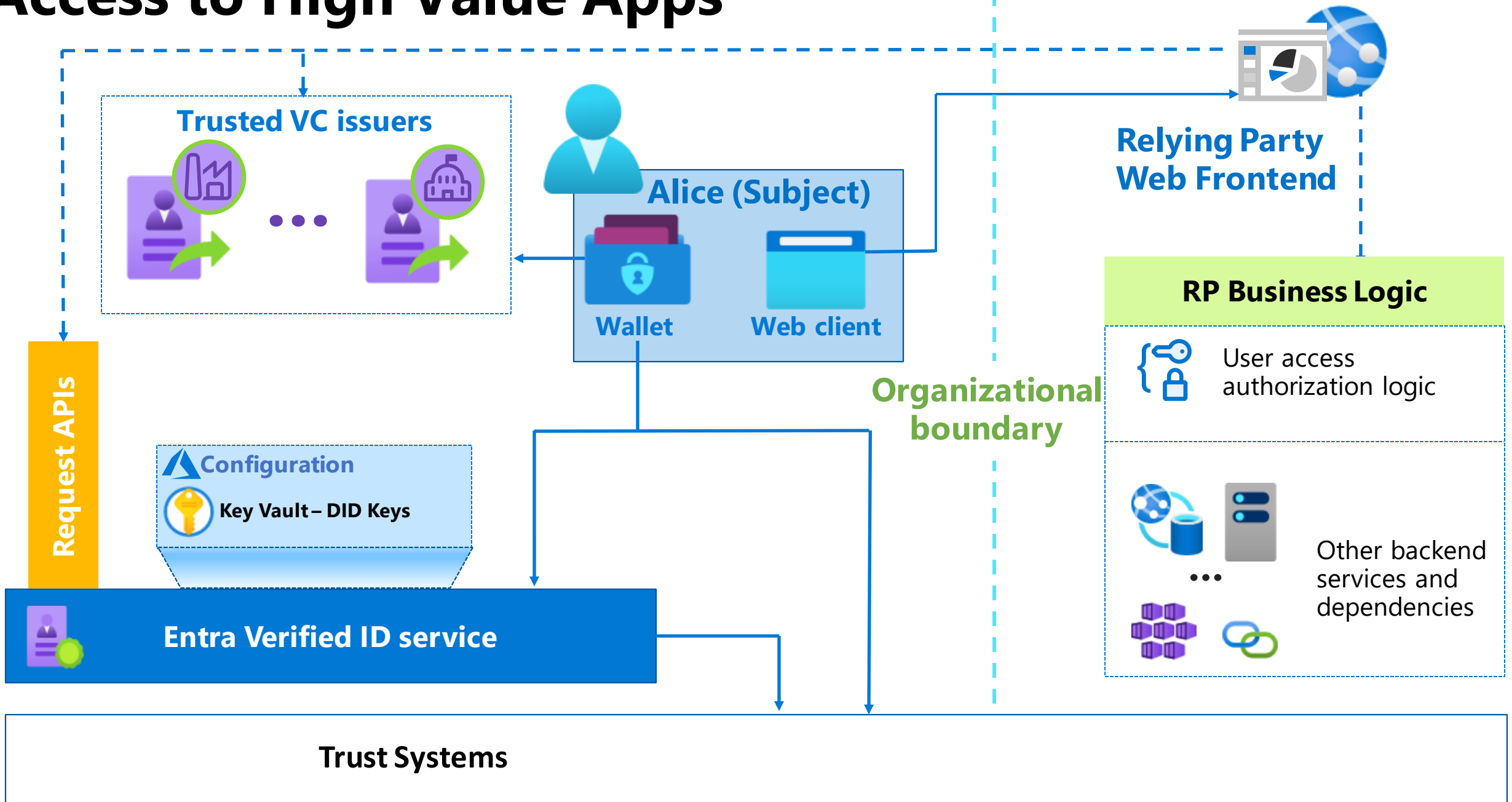


Building Blocks - Blueprints

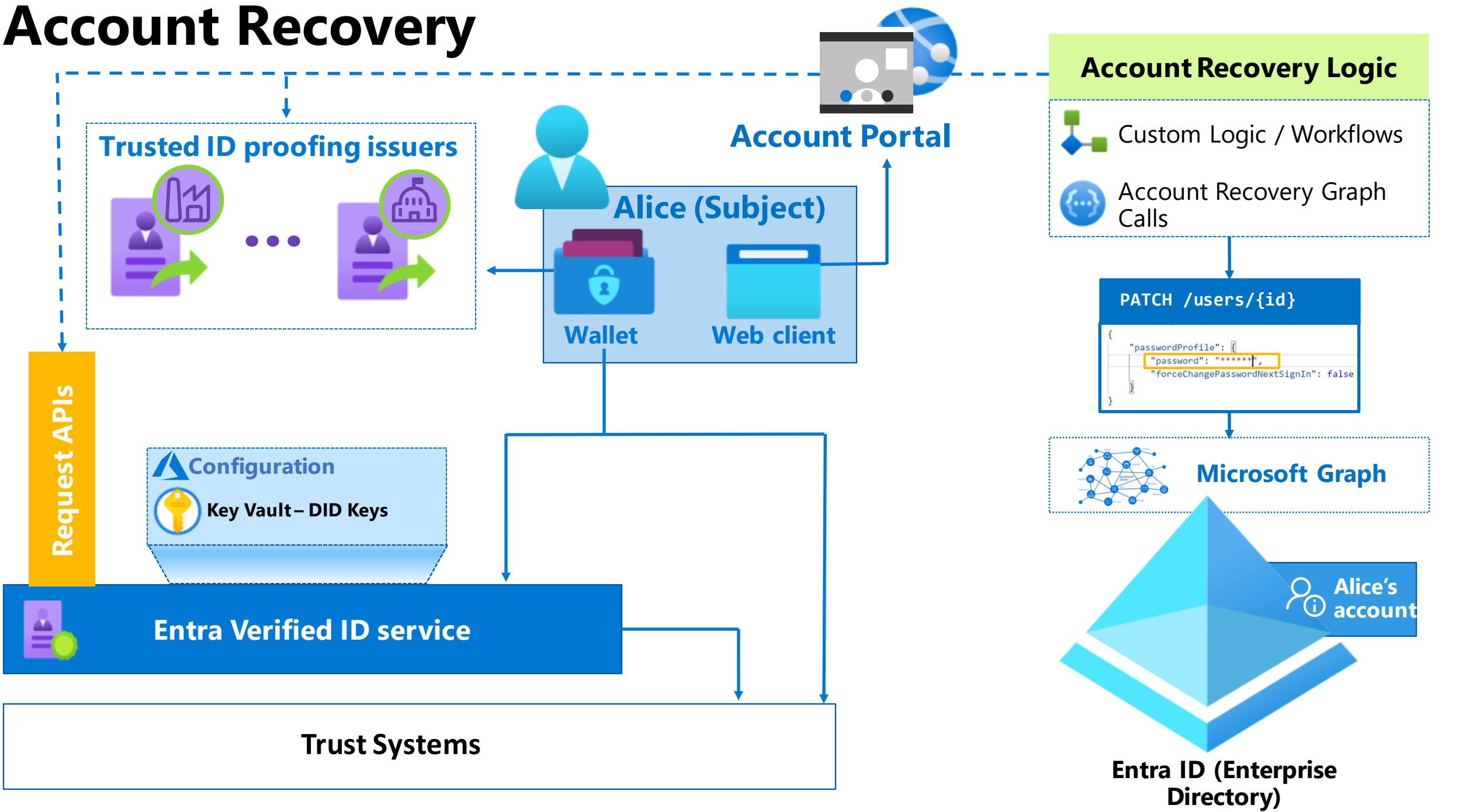
Account Onboarding












Access to High Value Apps



Account Recovery



Repository

 ARM	upd with new 1st party applds	4 months ago
 B2C	Rules & display updates for B2C	21 days ago
 CredentialFiles	Added VC input sample	6 days ago
 Postman	updated postman instructions and added admin API	last month
 ReadmeFiles	added QR code on signin page policy	2 months ago
 scripts/contractmigration	fix. added validityInterval and vc.type	24 days ago
 CODE_OF_CONDUCT.md	Initial CODE_OF_CONDUCT.md commit	2 years ago
 README.md	GA release	last month
 SECURITY.md	Initial SECURITY.md commit	2 years ago

GitHub Repo - <https://aka.ms/vcsample>

Verified ID: Scenarios

Hiring



- Identity verification
- Workplace credentials / employee ID
- Benefits onboarding
- Access

Worker Life



- Annual Benefits
- Employee Discounts
- Business to Business
- Business to Contractor

Alumni



- Last Day at Employer
- Alumni Benefits
- Proof of Employment
- List of Certifications

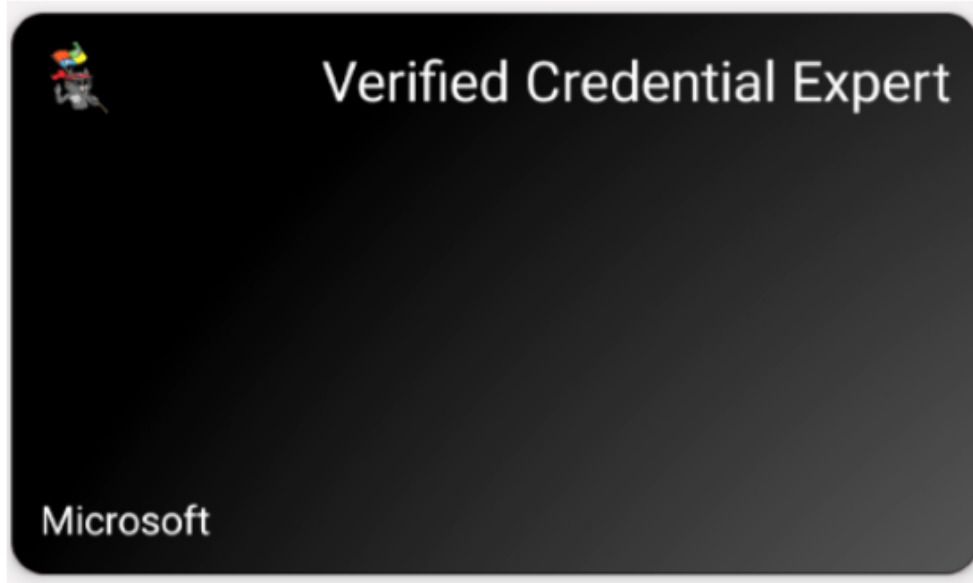
Verified ID: Scenarios

Worker Life



- Training/Licensing/Certs
- Cross Tenant access/managing customer environments
- Application Access
- Access to Conference/events/Projects

Sample Repository



There are several samples:

- [.NET](#)
- [Java](#)
- [Node](#)
- [Python](#)

Customer stories



Agilus and Credivera create a people-centric business by employing Microsoft Entra Verified ID



Condatis revolutionizes staff management with Microsoft Entra Verified ID



How a decentralized identity and verifiable credentials can streamline both public and private processes



UK Department for Education raises career potential for the next generation with Microsoft Entra Verified ID



RMIT future-proofs the university-to-student connection with Microsoft Entra Verified ID



Avanade reimagines access to training and skills management using Microsoft Entra Verified ID



University to enable students to securely manage their own transcripts with Verifiable Credentials



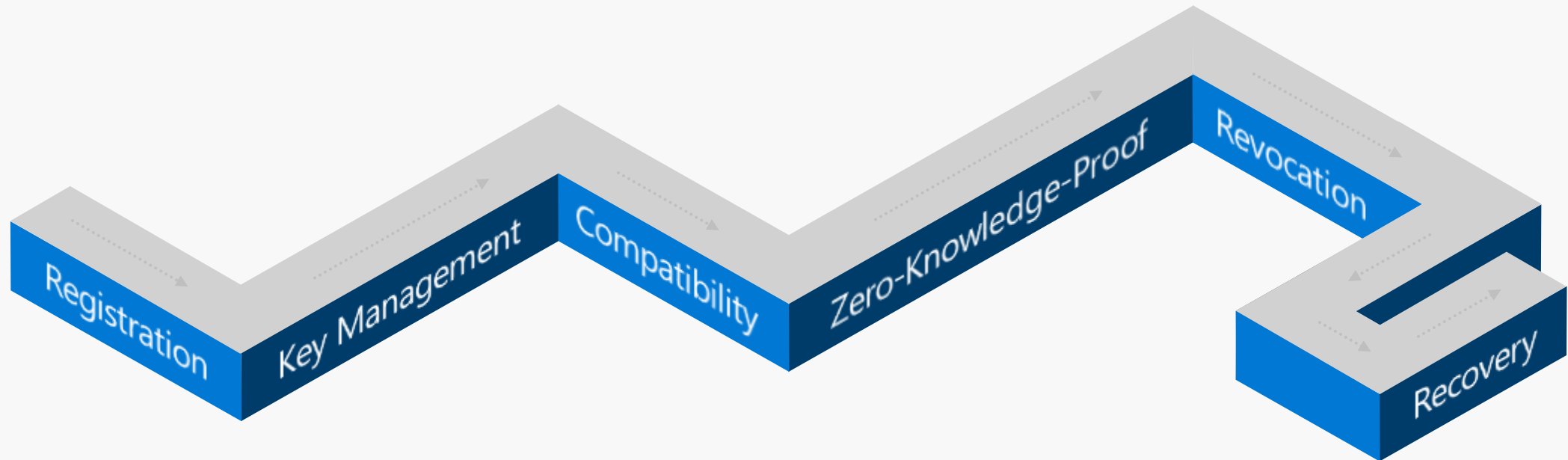
With high levels of security and trust, the NHS rapidly meets clinical demands using verified credentials

Next steps

The next 3 steps to making the ecosystem real

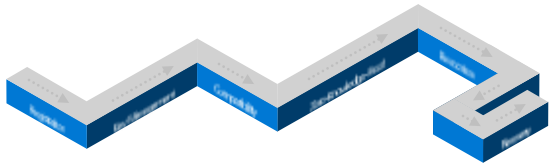
1. Ease of use

- ✓ Registration
 - ✓ Key management
 - ✓ Interoperability
- Recovery and revocation
- Selective Disclosure &
Zero-knowledge-proof



The next 3 steps to making the ecosystem real

1. Ease of use

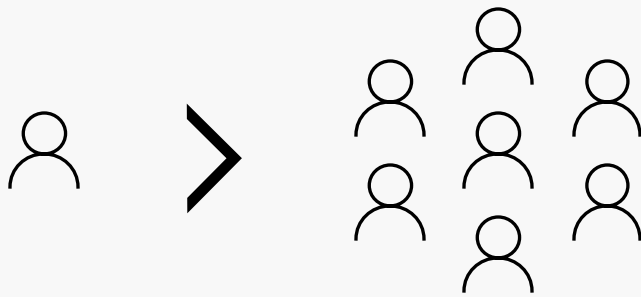


2. Performance & Scale

✓ DID:Web

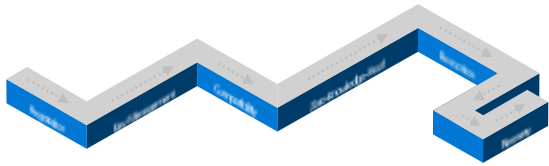
DID:ION (public preview)

Other methods?



The next 3 steps to making the ecosystem real

1. Ease of use



2. Performance & Scale



3. Join, collaborate, and contribute



Jumpstart with partners

Leading Identity verification partners



Accelerate adoption with a growing ecosystem of partner solutions



192 Countries

6000 Identification documents

1000's Organizational attributes

Millions Individual ID attributes

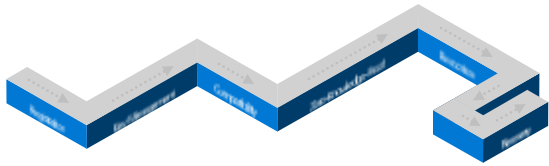
Decades of experience to go from idea to implementation in hours

Resources

1. <http://identity.foundation> Industry working group for all things Decentralized ID (DID)
2. <http://aka.ms/didwhitepaper> White paper by Microsoft: approach for DID + Verifiable Credentials
3. <http://aka.ms/didexplained> Quick overview
4. <https://youtu.be/Whc9Im-U0Wg> Overview for developers: scenario walk-through and how-to
5. <http://aka.ms/didfordevs> Developer documentation
6. Blogs ([scale and performance](#) and [self-owned key recovery](#))
7. <https://aka.ms/vcinterop> VC Interop profile
8. <https://aka.ms/diddemo> Demo site
9. <https://aka.ms/verifiedloyalty> - Microsoft Build session (wallet library)

The next 3 steps to making the ecosystem real

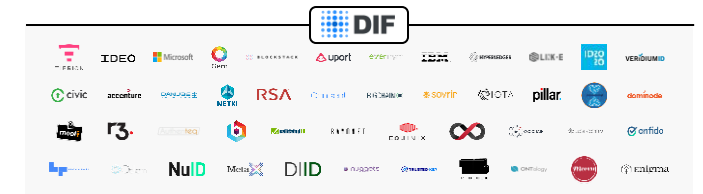
1. Ease of use



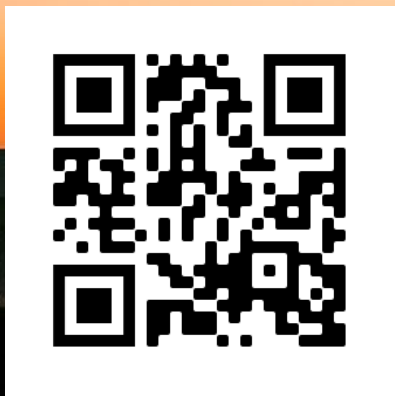
2. Performance & Scale



3. Join, collaborate, and contribute



Thank you.

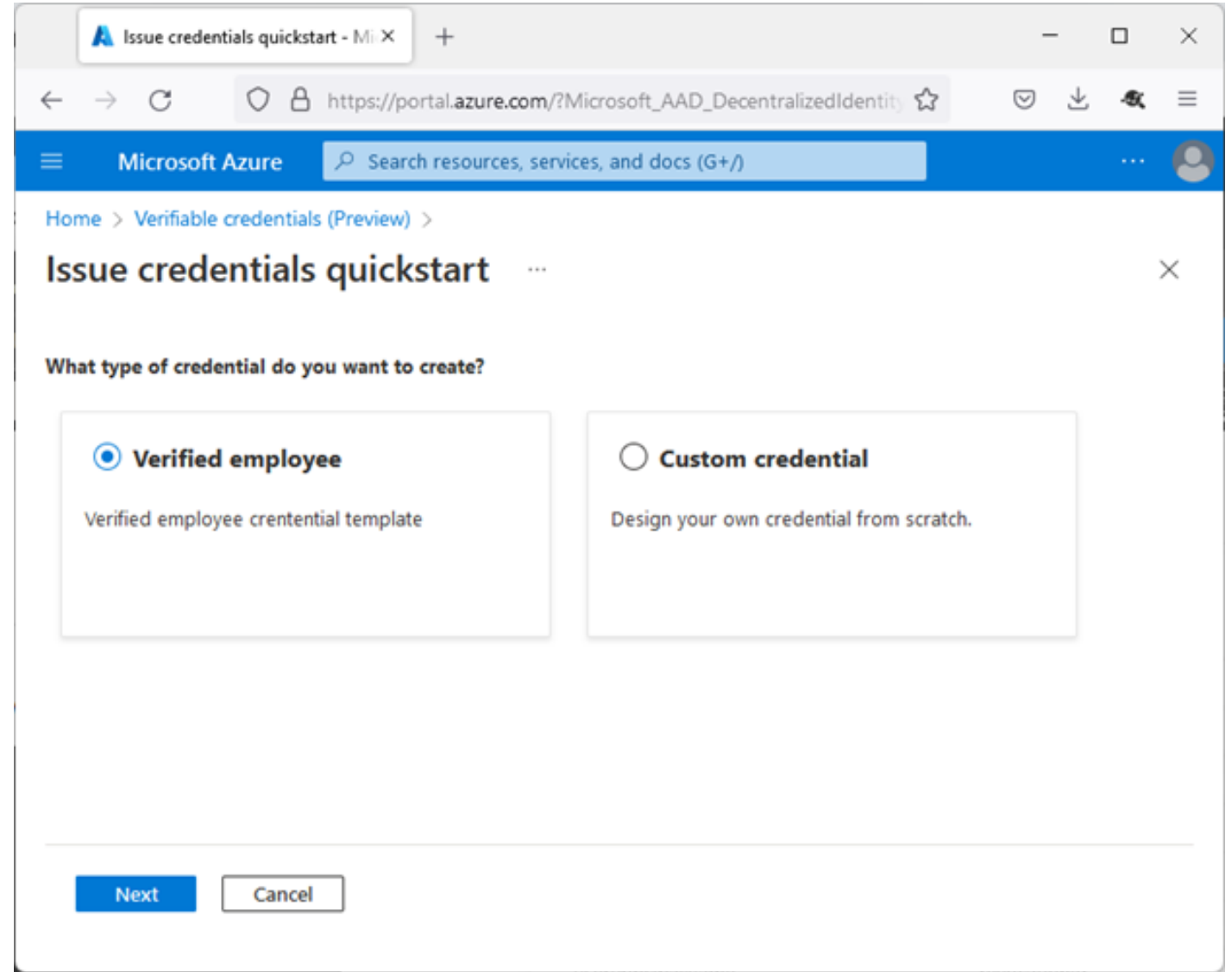


<http://aka.ms/vcdetails>

Thank you

Quickstart for Directory based claims

Effortlessly create a credential where the claims come from a user profile in the directory of the **Azure AD tenant**



The screenshot shows a web browser window with the title 'Issue credentials quickstart - Microsoft Azure'. The address bar displays the URL 'https://portal.azure.com/?Microsoft_AAD_DecimalizedIdentity'. The page header includes the 'Microsoft Azure' logo and a search bar. The breadcrumb navigation shows 'Home > Verifiable credentials (Preview) >'. The main heading is 'Issue credentials quickstart'. Below this, the question 'What type of credential do you want to create?' is displayed. There are two options: 'Verified employee' (selected with a radio button) and 'Custom credential' (unselected). The 'Verified employee' option includes the text 'Verified employee credential template'. The 'Custom credential' option includes the text 'Design your own credential from scratch.' At the bottom, there are two buttons: 'Next' (blue) and 'Cancel' (white).

Issue credentials quickstart - Microsoft Azure

https://portal.azure.com/?Microsoft_AAD_DecimalizedIdentity

Microsoft Azure Search resources, services, and docs (G+)

Home > Verifiable credentials (Preview) >

Issue credentials quickstart

What type of credential do you want to create?

☒ **Verified employee**
Verified employee credential template

☐ **Custom credential**
Design your own credential from scratch.

Next Cancel

Quickstart for Custom credentials

When using the Quickstart, just enter all details in the Azure portal and create a custom credential on a single page

Create a new credential - Micro: X

https://portal.azure.com/?Microsoft_AAD_Decimalized 90%

Microsoft Azure Search resources, services, and docs (G+ /)

Home > Verifiable credentials (Preview) > Issue credentials quickstart >

Create a new credential

Got feedback?

Create a custom credential that can be issued to your users. [Learn more](#)

Credential name *

A unique identifier for your credential, only displayed in the Azure Portal.

VerifiableCredentialExpert

Display file *

The display file describes the claims contained in the credential as well as the branding.

```
1 {
2   "locale": "en-US",
3   "card": {
4     "title": "Verified Credential Expert",
5     "issuedBy": "Microsoft",
6     "backgroundColor": "#000000",
7     "textColor": "#ffffff",
8     "logo": {
9       "uri": "https://didcustomerplayground.blob.core.w
10      "description": "Verified Credential Expert Logo"

```


[Learn how to create a display file](#)

Rules file *

The rules file determines what the user needs to do to get the credentials. Include an index claim if you want to be able to search for the credential later.

```
1 {
2   "attestations": {
3     "idTokens": [
4       {

```



This is what users will see in the Authenticator app. The card branding, title and color come from the display file. The acceptance requirements, such as 'sign in to your account' are covered by the rules file.

Microsoft Entra Verified ID Network

Search for published credential types and schemas in the Entra Verified ID Network to easily generate a presentation request

The screenshot shows the Microsoft Azure portal interface for setting up a verification request. The main heading is "Setup a verification request". Below it, there are tabs for "Select issuer(s)" and "Review". The "Select issuer(s)" tab is active, showing a table of issuers. The table has columns for "Issuer", "Linked domain", and "Credential type". The "Woodgrovedemo" issuer is selected, and the "VerifiedEmployee" credential type is chosen. The "Add" button is visible at the bottom right of the table.

Select issuer

Select an issuer of verifiable credentials from the Azure AD network. The choose which types of credentials to include in verification request.

Step 1 - Search/select issuers

Search for and select a verifiable credential issuer. Only issuers with verified domains will be searchable.

Issuer	Linked domain	Credential type
Woodgrovedemo	https://did.woodgrovedemo.com/	VerifiedEmployee

Step 2 - Select credential type(s)

Select the credential types to present to your user for verification.

<input type="checkbox"/>	BankofWoodgrovelidentity	givenName, familyName
<input checked="" type="checkbox"/>	VerifiedEmployee	displayName, givenName, jobTitle, preferredLanguage, surname, mail, revocationId, photo

Add

Verifying credentials using Microsoft Entra Verified ID Network